



INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 5 : G06K 19/06, G07F 7/10	A1	(11) International Publication Number: WO 92/16913 (43) International Publication Date: 1 October 1992 (01.10.92)
---	----	--

(21) International Application Number: PCT/GB92/00512

(22) International Filing Date: 20 March 1992 (20.03.92)

(30) Priority data:

9105851.1

20 March 1991 (20.03.91)

GB

(71) Applicant (for all designated States except US): THE SECURITY SYSTEMS CONSORTIUM LIMITED [GB/GB]; 60 Ebury Street, London SW1W 9QD (GB).

(72) Inventors; and

(75) Inventors/Applicants (for US only): BELL, Alan, J. [GB/GB]; 52 Laburnum Road, Fareham, Hampshire PO16 0SL (GB). BLOY, Colin, Henry [GB/GB]; 24A Sussex Heights, St Margarets Place, Brighton, East Sussex BN1 2FR (GB).

(74) Agent: GALLAFENT & CO; 8 Staple Inn, London WC1V 7QH (GB).

(81) Designated States: AT (European patent), AU, BE (European patent), CA, CH (European patent), DE (European patent), DK (European patent), ES (European patent), FR (European patent), GB (European patent), GR (European patent), IT (European patent), JP, LU (European patent), MC (European patent), NL (European patent), SE (European patent), US.

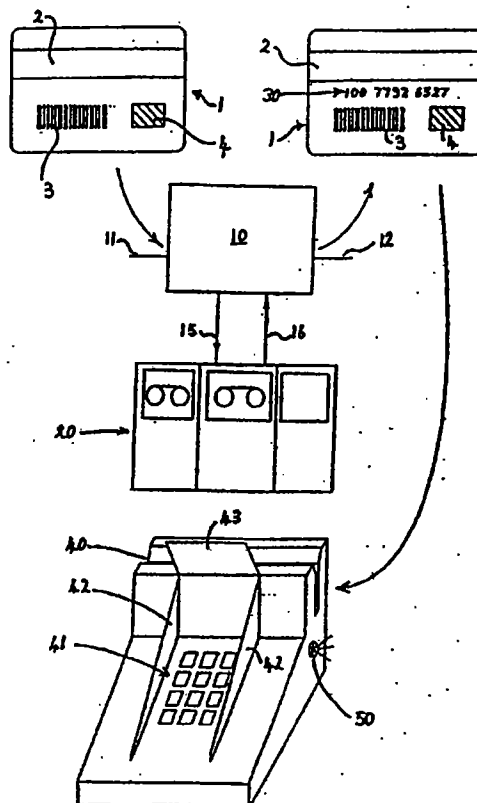
Published

With international search report.

(54) Title: SECURING FINANCIAL TRANSACTIONS

(57) Abstract

A system for securing financial transactions involving credit and charge cards is described. As well as the normal magnetic stripe (2), the card includes non visible coded information, for example an infra-red readable (but not human eye visible) bar code (3). When the card is personalised, data recorded on to magnetic stripe (2) may be combined with the bar code (3) and a randomly generated PIN number to produce check digits following a given algorithm. Those check digits can be recorded in the magnetic stripe (2). A stand alone validator i.e. not connected to a mainframe computer, can read both data from magnetic stripe (2) and the coded data such as bar code (3) and process the data and the PIN number input via a keypad (41) according to the algorithm to produce the check digits if they match, an indication validating the proposed transaction can be given, for example a green LED (50) lights up.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AT	Austria	FI	Finland	MI	Mali
AU	Australia	FR	France	MN	Mongolia
BB	Barbados	GA	Gabon	MR	Mauritania
BE	Belgium	GB	United Kingdom	MW	Malawi
BF	Burkina Faso	GN	Guinea	NL	Netherlands
BG	Bulgaria	GR	Greece	NO	Norway
BJ	Benin	HU	Hungary	PL	Poland
BR	Brazil	IE	Ireland	RO	Romania
CA	Canada	IT	Italy	RU	Russian Federation
CF	Central African Republic	JP	Japan	SD	Sudan
CG	Congo	KP	Democratic People's Republic of Korea	SE	Sweden
CH	Switzerland	KR	Republic of Korea	SN	Senegal
CI	Côte d'Ivoire	LJ	Liechtenstein	SU	Soviet Union
CM	Cameroon	LK	Sri Lanka	TD	Chad
CS	Czechoslovakia	LU	Luxembourg	TG	Togo
DE	Germany	MC	Monaco	US	United States of America
DK	Denmark	MG	Madagascar		
ES	Spain				

- 1 -

SECURING FINANCIAL TRANSACTIONS

This invention relates to securing financial transactions.

5

In recent years there has been a substantial move to cashless financial transaction using, as an essential element of the transaction, a plastics card. A variety of such cards, directed to use in differing types of financial transaction, has emerged. Mention may be made of credit cards, charge cards, cheque guarantee cards and cash cards.

10

15

20

Two main methods have emerged for the authentication of the card at the time of transaction. In the case of credit cards, charge cards and cheque guarantee cards, this is the signature of the user, which is applied to both the card (when the user initially receives it) and at the time of the transaction, either a credit or charge card voucher produced by the provider of goods or services at the time of the transaction, or a cheque form produced by the card holder in the case of a cheque guarantee card. The other method is use of a personal identification number (PIN number) known theoretically

- 2 -

only to the card holder and for use in cash card transactions. The requirement for a personal identification number arises from the majority of cash card transactions being effected via so called automated teller machines, which produce cash for the user without the cash dispenser being present in person in the form of a human cashier or teller.

When properly used, the PIN number approach provides a relatively high degree of security. Its use is however limited by the need to have the number checked and correlated with the data on the cash card at the time of the transaction. This is conventionally effected by connecting the automated teller machine on-line to a mainframe computer which, if a correct PIN number is provided by the user of the machine, authorises the transaction and enables the machine to dispense the cash.

While such a system is effective, it requires a very substantial investment in mainframe computer back-up and, for obvious reasons, tends to "fail safe" i.e. if the correct PIN number is not introduced, or if there is some other problem such as the misreading of magnetic data on the cash card, the transaction is simply blocked. While this is inconvenient to the user at the time, it generally inconveniences no-one else. Hold-ups, however, at other financial transaction processing stations, for example supermarket check-outs, which might be occasioned by a failed transaction of this nature, are unacceptable.

In situations such as supermarket check-outs, however, there is currently neither the equipment available to deal with on-line authentication nor would problems of delay be acceptable. Instead, authentication is effected

- 3 -

by signature. Despite the presumed uniqueness of signatures, they do not in fact work very well as a security measure. The standard problem with cheque guarantee cards is that, despite instructions to the contrary, users tend to keep them conveniently with their cheque books, and if both are stolen together the thief may well be able to learn a passable imitation of the signature on the card and then go out and make a substantial number of transactions over a short period of time before any alarm can be raised. This is clearly unsatisfactory.

The present invention seeks to provide an improved system using an improved form of card and novel authentication equipment.

According to a first general feature of the present invention there is provided on an authentication card having a magnetic strip with magnetically recorded data thereon, and additional coded marking which is invisible to the naked eye but machine-readable. This provides a first line of defence against card fraud if it is arranged that part of the data recorded magnetically and part of the invisibly recorded data are correlated in some way since then any magnetic tampering with the magnetically recorded data (which is often undertaken by professional thieves) will remove the correlation and enable a simple self-contained detector unit to show at the point of the transaction that the card has been tampered with.

Additionally, since the coded marking is invisible to the naked eye, it is not immediately apparent usually to the would-be card forger that the marking is there at all.

- 4 -

Although the marking is coded, for purposes which appear more fully below, the additional marking may also serve as a security feature merely by its presence. Thus if the additional marking is effected using a material
5 having certain physical characteristics and which is one not normally found in credit and charge cards, or one the synthesis of which is difficult to achieve, a forged card may be distinguished from a genuine merely by the presence of the material making up the coded marking.

10

As noted above, the data on the magnetic strip and the data in the additional coded marking may be directly correlated to enable simple detection of tampering of the magnetic data. However, a major advantage of the present
15 invention is that such data as is coded in the magnetic strip and the coded marking may be correlated via a PIN number known to the holder of the card but apparent from neither the magnetic data nor the invisible data.

20 Using a card coded in this way, it is possible to authenticate a transaction without the necessity of referring to a mainframe computer but with a very high degree of certainty by reading data from the card, both the magnetic data and the non-visible data, and
25 correlating that data with a PIN number provided by the card holder at the time of the transaction. The PIN number may be inserted into the detector unit by the card holder in a fashion which does not reveal the PIN number to the bystander, or for example the cashier, at the
30 vending establishment.

A detector unit may be used to validate the transaction. Thus according to a further feature of the present invention there is provided validation apparatus for use

- 5 -

with a card of the type described above which comprises means for reading data recorded magnetically on a magnetic strip of the card, means for reading data from the additional coded marking thereon, personal

5 identification number input means, a pre-programmed processing unit adapted to process data input from the magnetic strip coded marking and PIN number inputs and to display the results of such processing as a visual indication corroborating or denying the validity of a
10 proposed transaction.

Such validator apparatus may be embodied in a relatively small, relatively inexpensive unit. So called swipe readers for cards bearing a magnetically coded stripe are
15 well known and find application in numerous areas of technology, for example in electronic tills and card operated telephone boxes. They usually include a channel along which the card is passed, either by hand or driven by appropriate machinery, so that the magnetic stripe on
20 the card passes over a magnetic reading head.

Conveniently the invisibly coded marking on the card can be read at the same time, this generally implying that the coded marking extends linearly in a direction parallel to that of the magnetic stripe. A preferred
25 marking is a bar code type marking which is easily applied during manufacture of the card. The bar code marking may be on the same side of the card as the magnetic stripe or on the opposite side and the swipe reader will need to be constructed accordingly.
30

As noted above, the additional coded marking on the card is invisible to the naked eye. This can be effected by a variety of means, preferred systems being to incorporate the marking in the interior of the card. The marking may

- 6 -

be effected in a material which is itself effectively invisible (transparent or the same colour as the material of card) or it may be made in a material which when directly viewed is visible but which is rendered
5 invisible by being covered with an opaque layer rendering it invisible to the human eye but where the opaque layer is not opaque to some appropriate form of sensing. For example the code may be printed using a material giving a detectable infra-red absorption or reflectance but
10 covered by a material transparent to infra-red radiation but opaque to the human eye. Putting the marking in the interior of the card also makes it much more difficult for a person who wishes to commit fraud by using a stolen card to change the data on the card.

15 Thus a particularly preferred form of card in accordance with the present invention is a plastics card having, printed in the interior thereof, a marking readable at non-visible wavelengths, preferably at infra-red
20 wavelengths, the marking being located between a plastics card base and a cover laminated to the base and transparent to the wavelength at which the bar code is readable.

25 The invention as illustrated by way of example in the accompanying drawing which shows diagrammatically card manufacture and transaction validation using the card.

30 Referring to the drawing this shows at the top left a stylised credit card 1 which may be of standard shape and size. On one side of the card is a magnetic stripe 2 of standard construction. Also printed on the card is a bar code 3 and a patch 4. Bar code 3 and patch 4 may be made of the same material or may be different.

- 7 -

Although barcode 3 is shown on the drawing for clarity visibly, it may be printed in a material visually indistinguishable from the background. Barcode 3 and patch 4 may be printed on the card base and then covered with, for example, a visually opaque, infra-red transparent cover sheet.

The bar code 3 and patch 4 may be printed on the card or on a layer making up the card by any convenient means. Ink jet printing of bar codes is a convenient and inexpensive means of printing bar codes on successive cards which vary from card to card. This is important for reasons indicated below.

Cards of the type illustrated in the top left of the accompanying drawing, and including e.g. printing with graphic material indicative of the intended card issuer are produced by standard mass production processes. However for use, cards must carry data personal to the user. Standard machines are accordingly available in commerce for processing pre-manufactured cards to personalise them. A typical such machine is commercially available under the trade designation Datacard 4650 from Data Card Limited and its affiliates. Other card embossing and recording systems are available from other manufacturers.

In the drawing, such a machine is represented diagrammatically by box 10 having an input tray 11 for cards to be personalised and an output delivery 12 where cards which have been processed collect.

The card embossing and recording system 10 is connected via a suitable data transmission links 15 and 16 with a

- 8 -

mainframe computer schematically indicated at 20 and under the control of the card issuer, for example a bank, finance company or the like.

- 5 Card personalisation is now effected by the embossing and recording system 10 as follows:

10 The invisible bar code 3 is read by a suitable reader within unit 10. This is fed via data transmission line 15 to the mainframe computer 20 together with a request to provide data to be put on the card. Thus the mainframe computer may be requested to provide the embossing and recording system with the account number name and details of the intended card holder. This is 15 then transmitted from the mainframe computer 20 to the embossing and recording system 10 via data link 16.

20 In accordance with the invention, the mainframe computer which receives the data as to the bar code 3, carries out suitable mathematical processing on the number represented by the bar code and on other numbers associated with the particular account or person to whom the card will be issued. The mathematical process or algorithm used may vary widely but is used to combine the 25 invisible number from bar code 3 with data e.g. from the person's account number, and with a randomly generated PIN number which will be assigned to the cardholder. For example one form of mathematical processing may be to take the number represented by the bar code 3, add the 30 person's account number to it, multiply that sum by the randomly generated PIN number and discard all but the last three digits of the resulting large number. Those three digits can then be regarded as a checking number which is then fed back via data link 16 to the embossing

- 9 -

and recording system 10. The embossing and recording system may be arranged to record those three digits on to the magnetic stripe 2.

5 The top right hand corner of the drawing shows diagrammatically the card after processing. It still has unchanged bar code 3, patch 4 and magnetic stripe 2. However the cardholder's account number 30 has been embossed thereon and is shown and this number and the
10 check digits are recorded on magnetic stripe 2. The card may also be appropriately embossed or otherwise identified e.g. with the name of the cardholder and an expiry date.

15 The so processed card can then be transmitted to the cardholder in the usual way while the mainframe computer 20 (which of course knows the PIN number allotted to that customer) may generate a separate letter which the computer separately despatches to the cardholder advising
20 him or her of the PIN number he or she has been assigned.

Once the cardholder is in possession of the card, it can be used in the normal way. Although this is not indicated for the sake of clarity and drawing, the card
25 may include a conventional signature strip and may be validated by signature comparison or using some form of on-line validation as is well known. However, because of the presence of bar code 3 in the card and patch 4 further means of validation are now available.

30 The bottom of the attached drawing shows diagrammatically a self contained validator unit which may be located at any appropriate transaction processing station for example in a store, supermarket, restaurant or the like.

- 10 -

This unit has a slot 40 through which the card 1 may be swiped. Located either side of slot 40 within the validator unit are appropriate sensors for reading magnetic data on magnetic stripe 2 and the coded data on bar code 3. Patch 4 may be used in conjunction with the bar code to facilitate reading. For example if patch 4 is of known width, the amount of time patch 4 is under a detector head may give an indication of appropriate clocking speed for reading the bar code, thus compensating for different swipe speeds.

In practice, the card is first swiped through the slot 40 and the cardholder is then invited to input his or her PIN number via a conventional keypad 41. Keypad 41 is surrounded by screens 42,43 in order to minimise the chance of the PIN number being detected by a casual observer. There is no display of what PIN number has been entered but within the cabinet of the validator unit which includes slot 40 is an appropriately programmed integrated circuit. This is arranged to receive data read from the card and data input from the keypad 41 and then to take the data read from the card (the account number from magnetic stripe 2 and the bar code 3) and combine it in the same way as the mainframe computer 20 did when the card was being personalised, to generate a large number and therefor the three check digits by the system explained above. The circuit also contains comparison means to determine whether the three check digits so generated match the three check digits read from magnetic stripe 2. If they do, an indicator such as a bright light emitting diode 50 located on the side of the validator unit lights up green thus enabling the proposed transaction to be authorised while if they do not match, diode 50 lights red.

- 11 -

It can be seen from the above that validation is essentially carried out by the checking process indicated and using the appropriate algorithm. There is no need to refer to a mainframe computer.

5

The validator unit shown at the bottom of the drawing may simply act as a transaction validator as indicated above or it may be more sophisticated. For example it may include large quantities of electronic memory enabling it to record details of each transaction for example the date the identity of the checkout store and perhaps of the checkout operator and perhaps other data enabling tracing to be carried out if it is subsequently decided that a use of particular card needs to be traced. The circuitry within the unit may also for example incorporate programming enabling detection of operation at unusual hours or to enable an unusual pattern of operation to be detected, for example if repeated attempts are made to validate the same card using a succession of different PIN numbers as would occur if a member of a supermarket staff who had picked up a lost card but not declared that tried to find the PIN number related to that card by repeated trial and error.

10

15

20

25

30

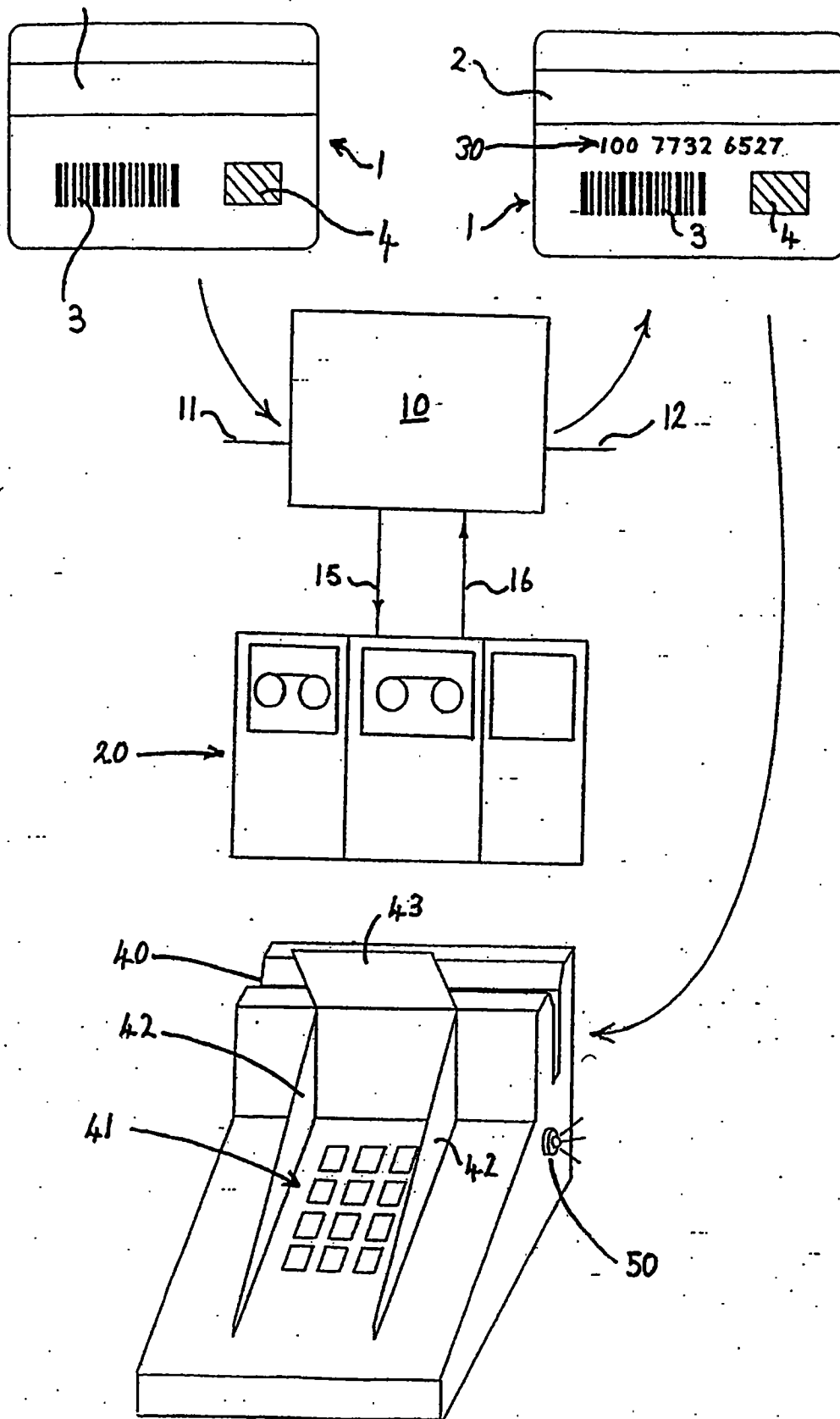
The validator unit may of course have means enabling it to be programmed or reprogrammed or enabling material stored by it to be downloaded for subsequent investigative processing. The unit must of course be rendered reasonably secure against tampering by any appropriate means including for example means erasing its programming if the casing is opened by an unauthorised person.

CLAIMS

1. An authentication card for securing financial transactions consisting of a card base, a magnetic strip having magnetically recorded data thereon and characterised by an additional coded marking invisible to the naked eye but machine-readable.
2. An authentication card according to Claim 1, wherein the additional coded marking is in the form of a bar code.
3. An authentication card according to Claim 1 or 2, wherein the additional coded marking is readable using infra-red radiation.
4. An authentication card according to any one of Claims 1 to 3, wherein the magnetic strip contains as part of the magnetically recorded data a plurality of check digits obtained by applying an algorithm to other data recorded on the magnetic strip and the additional coded marking.
5. Validation apparatus for use with an authentication card and in accordance with any one of the preceding claims and including means for reading data recorded magnetically on the magnetic strip on the card and means for inputting a personal identification number, and characterised by means for reading the data from the additional coded marking on the card and by a pre-programmed processing unit adapted to process data input from the magnetic stripe coded marking, the PIN number input and the additional coded marking and adapted to compare the results of

such processed data with data also recorded magnetically on the magnetic strip and display the results of such comparison.

- 5 . 6. Validation apparatus according Claim 5 and including a channel along which the card may be moved, a magnetic reading head adapted to read data from the magnetic stripe thereon and characterised by means for reading the additional coded marking thereon.



INTERNATIONAL SEARCH REPORT

International Application No.

PCT/GB 92/00512

I. CLASSIFICATION OF SUBJECT MATTER <small>Of several classification symbols apply, indicate all *</small> According to International Patent Classification (IPC) or to both National Classification and IPC IPC ⁵ : G 06 K 19/06, G 07 P 7/10		
II. FIELDS SEARCHED Minimum Documentation Searched ¹		
Classification System	Classification Symbols	
IPC ⁵	G 06 K, G 07 P	
Documentation Searched other than Minimum Documentation to the extent that such documents are included in the fields searched ²		
III. DOCUMENTS CONSIDERED TO BE RELEVANT³		
Category ⁴	Citation of Document, ⁵ with indication, where appropriate, of the relevant passages ¹²	Relevant to Claim No. ¹³
X	DE, C2, 3 013 211 (GAO) 24 August 1989 (24.08.89), see the whole document; especially column 2, lines 40-49; column 3, line 47 - column 4, line 18; claim 1; fig. 2; position 26,7.	1,4,5, 6
Y	---	2
Y	US, A, 4 114 033 (OKAMOTO) 12 September 1978 (12.09.78), see claim 1; fig. 1.	2
A	DE, A1, 2 901 521 (DATASAB) 26 July 1979 (26.07.79), see the whole document; especially claims 1,7.	1,5
<p>[*] Special categories of cited documents: ¹⁴</p> <p>"A" document defining the general state of the art which is not considered to be of particular relevance</p> <p>"E" earlier document but published on or after the international filing date</p> <p>"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)</p> <p>"O" document referring to an oral disclosure, use, exhibition or other means</p> <p>"P" document published prior to the international filing date but later than the priority date claimed</p> <p>"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention</p> <p>"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step</p> <p>"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.</p> <p>"Z" document member of the same patent family</p>		
IV. CERTIFICATION		
Date of the Actual Completion of the International Search 18 May 1992		Date of Mailing of this International Search Report 11.06.92
International Searching Authority EUROPEAN PATENT OFFICE		Signature of Authorized Officer Nicole De Bie

ANHANG

ANNEX

ANNEXE

zum internationalen Recherchen-
bericht über die internationale
Patentanmeldung Nr.

to the International Search
Report to the International Patent
Application No.

au rapport de recherche inter-
national relatif à la demande de brevet
international n°

PCT/GB 92/00512 SAE 57794

In diesem Anhang sind die Mitglieder
der Patentfamilien der in obenge-
nannten internationalen Recherchenbericht
angeführten Patentdokumente angegeben.
Diese Angaben dienen nur zur Unter-
richtung und erfolgen ohne Gewähr.

This Annex lists the patent family
members relating to the patent documents
cited in the above-mentioned inter-
national search report. The Office is
in no way liable for these particulars
which are given merely for the purpose
of information.

La présente annexe indique les
membres de la famille de brevets
relatifs aux documents de brevets cités
dans le rapport de recherche inter-
national visé ci-dessus. Les renseigne-
ments fournis sont donnés à titre indica-
tif et n'engagent pas la responsabilité
de l'Office.

In Recherchenbericht angeführtes Patentdokument Patent document cited in search report Document de brevet cité dans le rapport de recherche	Datum der Veröffentlichung Publication date Date de publication	Mitglied(er) der Patentfamilie Patent family member(s) Membre(s) de la famille de brevets	Datum der Veröffentlichung Publication date Date de publication
DE C2 3013211	24-08-89	BE A1 888254	31-07-81
		CH A 656243	13-06-86
		DE A1 3013211	08-10-81
		FR A1 2480009	09-10-81
		FR B1 2480009	31-01-86
		GB A1 2073461	14-10-81
		GB B2 2073461	15-02-84
		JP A2 56157551	04-12-81
		JP B4 1043343	20-09-89
		SE A 8102026	04-10-81
		SE B 454392	25-04-88
		SE C 454392	04-08-88
US A 4114033	12-09-78	keine - none - rien	
DE A1 2901521	26-07-79	AT A 423/79	15-03-88
		AT B 386903	10-11-88
		BE A1 873587	16-05-79
		DE C2 2901521	08-06-89
		DK A 224/79	20-07-79
		DK B 152865	24-05-88
		DK C 152865	10-10-88
		ES A1 483966	01-04-80
		ES A5 483966	12-04-80
		ES A1 476979	16-06-80
		ES A5 476979	25-06-80
		FI A 790170	20-07-79
		FI B 73842	31-07-87
		FI C 73842	09-11-87
		FR A1 2415340	17-08-79
		FR B1 2415340	19-09-86
		GB A1 2013009	01-08-79
		GB B2 2013009	10-03-82
		IT A0 7919447	19-01-79
		IT A 1109496	16-12-85
		NL A 7900413	23-07-79
		NO A 790134	20-07-79
		NO B 161407	02-05-89
		NO C 161407	09-08-89
		SE A 7900473	20-07-79
		SE B 442457	23-12-85
		SE C 442457	10-04-86
		US A 4214230	22-07-80